THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Mo., as second-class matter.

VOL. VII. DECEMBER, 1900. No. 12.

SOME METHODS OF CONSTRUCTING SUBSTITUTION GROUPS.

By DR. G. A. MILLER, Cornell University, Ithaca, N. Y.

We have observed that the first n powers of a circular substitution of degree n constitute a group of order n. If a substitution is composed of more than one cycle its order is the least common multiple of the degrees of all its cycles. This is also the order of the group which it generates. Any group which is generated by a single substitution is called *cyclical.* A cyclical group is clearly abelian but an abelian group is not necessarily cyclical. *There is one and only one cyclical abstract group of every possible order n* since the combinatory laws of such a group are the same as those of the roots of the equation $x^n=1$, where n is any positive integer. The only orders of which there is no group except the cyclical are those which are not divisible by the square of a prime and do not contain any prime factor which is congruent to 1 with respect to another prime factor as modulus. The composite orders below 100 that have this property are 15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95.

Let S and T represent any two commutative substitutions. This property is expressed by each of the following three equivalent equations :

$$ST=TS \qquad T^{-1}ST=S \qquad T=S^{-1}TS$$

where T^{-1} and S^{-1} indicate the inverse of T and S, respectively; *i. e.* $T^{-1}T=1=S^{-1}S$. In general $T^{-1}ST$ is called the transform of S with respect to T. All the substitutions of degree m that are commutative with any given substitution T

of degree n form a group, for if S_1 and S_2 are commutative with T then will S_1^2, S_2^2, S_1S_2, S_2S_1 have the same property.* By raising both members of the equation $S^{-1}TS=T$ to the β power we have

$$S^{-1}TS.S^{-1}TS.S^{-1}TS\ldots.=T^\beta \text{ or } S^{-1}T^\beta S=T^\beta .$$

Hence every substitution that transforms T into itself must transform each of the substitutions of the group generated by T into itself. When T consists of a single cycle m cannot be less than n,† and when $m=n$ all the substitutions that are commutative with T are the n different powers of T; for if some other substitution of degree n would transform T into itself its product into some power of T would give a substitution of degree less than n that would also transform T into itself.

If T consists of β cycles of degree $n\div\beta$ (in this case T is said to be a regular substitution) the order of the group of degree n which is formed by all the substitutions that are commutative with T is $\left(\frac{n}{\beta}\right)^\beta.\beta\,!$ since the β cycles are permuted according to the symmetric group of degree β. In general, let T contain a_1 cycles each of degree a_2, b_1 cycles each of degree b_2, ...; then the order of the group which is formed by all the substitutions of degree n that are commutative with T is $a_2^{a_1}.a_1!.b_2^{b_1}.b_1!\ldots.$ In particular, when no two cycles of T are of the same degree the order of this group is the product of the degrees of these cycles, and the necessary and sufficient condition that the powers of T include all the substitutions of degree n that are commutative with T is that the degree of each cycle of T is prime to that of every other cycle. When $m=n+\alpha$ $(\alpha>1)$ the required group is obtained by multiplying the given group of degree n by the symmetric group of order $\alpha\,!$

We have now considered the groups which are formed by all the substitutions which are commutative with a given substitution T; *i. e.* by all the values of S which satisfy the equation $S^{-1}TS=T$. This is a special case of the problem to find all the groups which are formed by all the values of S which satisfy the equation $S^{-1}TS=T$.

By raising both members of this equation to the β power we obtain $S^{-1}T^\beta S=T^\beta=(T^\beta)^\alpha$; *i. e. if a substitution transforms T into a certain power it transforms all the substitutions of the group generated by T into the same power*, and hence it must transform this group into itself. Since all the substitutions which transform a group into itself must form a group all the values of S which satisfy the equation $S^{-1}TS=T^\alpha$, α having every possible value, constitute a group (G) whose order we proceed to determine.

From $(S^{-1}TS)^\alpha=S^{-1}T^\alpha S$ and $S^{-1}\mid S=1$ it follows that a transform of T cannot be of a higher order than T, and from $S^{-1}T^\alpha S=1$ we have $T^\alpha S=S$ or

*Cf. Burnside, *Theory of Groups*, 1897, page 215.

†It will be assumed throughout that the substitutions of degree m which are commutative with T involve no elements except those contained in T whenever m is equal to or less than n. When m is greater than n these substitutions are supposed to include all the elements of T.

$T^a=1$; *i. e.* a transform of T cannot be of a lower order than T. Since the order of any transform of T is equal to the order of T it follows that α must be prime to the order of T in $S^{-1}TS=T^a$. By writing any such power of T below T we can at once write down the substitution which transforms T into this power. Hence α can have all the values that are prime to the order of T. To complete the determination of the order of G it is desirable to arrange its substitutions in a rectangular form, as follows :*

$$
\begin{array}{llll}
1 & s_1 & s_2 \ldots\ldots\ldots s_{l-1} \\
t_1 & s_1 t_1 & s_2 t_1 \ldots\ldots s_{l-1} t_1 \\
t_2 & s_1 t_2 & s_2 t_2 \ldots\ldots s_{l-1} t_2 \\
\cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot \\
t_{k-1} & s_1 t_{k-1} & s_2 t_{k-1} \ldots s_{l-1} t_{k-1}
\end{array}
$$

The first row contains all the substitutions which transform T into itself and hence forms a subgroup of G. It is supposed that each t is so selected that it does not occur in any row that precedes it. Since the first row includes all the substitutions of G that transform T into itself $t_1^{-1}Tt_1=T^{a_1}$ (α_1 is not equal to 1). Hence $(s_a t_1)^{-1}Ts_a t_1=t_1^{-1}s_a^{-1}Ts_a t_1{}^*=t_1 Tt_1=T^{a_1}$ ($\alpha_1=0, 1, 2, \ldots, l-1$); *i. e.* each of the substitutions of the second row transforms T into T^{a_1}. G cannot contain any other substitution h which has this property for by transforming by t_1^{-1} each member of the equation $h^{-1}Th=T^{a_1}$ we have $(ht_1^{-1})^{-1}Tht_1^{-1}=t_1T^{a_1}t_1^{-1}=T$. From the fact that $ht_1^{-1}=s_a$ it follows that $h=s_a t_1$. No two of the substitutions of the second row are identical for from $s_a t_1=s_\beta t_1$ there results $s_a t_1 t_1^{-1}=s_\beta t_1 t_1^{-1}$ or $s_a=s_\beta$. The number of substitutions that transform T into T^{a_1} is therefore equal to l, the number that are commutative with T. The order of G is then kl, k being equal to the number of positive integers less than the order of T and prime to it.

Having determined the order of the groups which are composed of all the substitutions that are commutative with a given substitution T or with the group generated by T, we proceed to determine some of the properties of these groups. We first observe that when T is regular the group which is composed of all the substitutions which transform T into itself contains no selfconjugate substitutions except the powers of T. Since such a group contains the product of all the cycles of T a selfconjugate subgroup could not permute any of the cycles of T, and among the substitutions that do not permute any of these cycles the powers of T are clearly the only ones that are selfconjugate. This fact leads to the following interesting result : *The necessary and sufficient condition that the group of degree n which is composed of all the substitutions which are commutative to T is*

*This arrangement seems to have been first employed by Abbati in 1802, *Burkhardt, Zeitschrift fur Mathematik und Physik*, Vol. 37, page 141. By means of it we can see directly that the order of any subgroup is a divisor of the order of the group.

†$(t_1 t_2 \ldots t_r)^{-1}=t_r^{-1}\ldots t_2^{-1}t_1^{-1}$ since $t_1 t_2 \ldots t_r t_r^{-1}\ldots t_2^{-1}t_1^{-1}=1$.

conjugate to that which is composed of all the substitutions that are commutative to T' is that T and T' are conjugate.*

When an element of a substitution is replaced by itself it is said to form a cycle of a single element. *E. g.* the substitution $abc.de$ is said to consist of two cycles if it is regarded as a substitution of degree five. If it is regarded as a substitution of degree six it is said to consist of three cycles, etc. According to this definition of cycle the product of any substitution s and a transposition† t involves either one more cycle or one less cycle than s. First suppose that the elements of t are found in two cycles of s and that each of these cycles begins with an element of t. It is clear that st contains a single cycle which includes all the elements of these two cycles and hence st has one less cycle than s. The other possibility is that the two elements of s are found in the same cycle of s and we may suppose that this cycle c begins with one of these elements. Let $c=a_1 \ldots . a_\alpha \ldots . a_\beta$ and $t=a_1 a_\alpha$ then will $ct=a_1 \ldots . a_{\alpha-1} . a_\alpha \ldots . a_\beta$, the subscripts of the elements of c being arranged in ascending order and $\alpha \geqq 2$, $\beta \geqq \alpha$. Hence we observe that in this case st contains one more cycle than s.

Any cycle and hence any substitution can be represented as the product of a series of transpositions in an infinite number of ways. For instance, $c=a_1 a_2 a_3 \ldots . a_l = a_1 a_2 \times a_1 a_3 \times \ldots . \times a_1 a_l = a_1 a_3 \times a_3 a_2 \times a_1 a_4 \times \ldots . a_1 a_l =$ etc.

By means of the results in the preceding paragraph we can readily prove that the numbers of these transpositions, for a given substitution s, are either all odd or all even. For, let $s=t_1 t_2 \ldots . t_r$, $t_1, t_2, \ldots ., t_r$ being transpositions. Then will $st_r \ldots . t_2 t_1 = 1$. If γ is the number of cycles of s and n its degree the first member of the last equation involves $n-\gamma$ more cycles than s. Hence $r-(n-\gamma)$ must be even; *i. e.* if one of the two numbers r, $n-\gamma$ is even the other is even also. Since the latter of these numbers is fixed when the substitution is given the theorem‡ is proved. Incidentally we observe that $n-\gamma$ is the smallest number of transposittons whose product is a substitution of degree n and γ cycles and that $r-(n-\gamma)$ can be made equal to any even integer. s is called positive or negative as r is even or odd.

Since the product of two positive substitutions is positive it follows that every group which involves negative substitutions must contain a subgroup composed of its positive substitutions. The order of this subgroup is half the order of the entire group since the product of a positive and a negative substitution is negative and the product of two negative substitutions is positive. The group which is composed of all the positive substitutions of degree n is called the alternating group of order $n! \div 2$. If a subgroup is transposed into itself by all the substitutions of the entire group it is called *selfconjugate.* A subgroup which includes half the substitutions of a group must be either selfconjugate or one of two conjugate subgroups. The latter is impossible since all the substitutions of one

*Two substitutions, or groups, are conjugate when one is the transform of the other.

†A transposition is a substitution of degree two; *e. g.*, ab, cd, ...

‡For a different proof of this fundamental theorem see Burnside, *Theory of Groups*, 1897, page 9; Cole's edition of *Netto's Theory of Substitution*, 1892, page 17; etc.

of these conjugates would have to transform the other into itself for a substitution must transform every subgroup in which it occurs into itself.

While every subgroup whose order is half the order of the group is self-conjugate a subgroup of any lower order need not be self-conjugate. If a group contains a subgroup of one-third its order that is not selfconjugate it must contain three subgroups of this order which are transformed according to the symmetric group of order six by all the substitutions of the group.

AN ELEMENTARY EXPOSITION OF GRASSMANN'S "AUSDEHNUNGSLEHRE," OR THEORY OF EXTENSION.

By JOS. V. COLLINS. Ph. D., Stevens Point, Wis.

[Concluded from November Number.]

APPLICATION TO MECHANICS.

168. A force is completely represented by a point vector. We will denote a force by $F\rho$, where F denotes the length and direction of a vector, indicating respectively the intensity and direction of the force, and ρ is the point of application. It is apparent here that two letters are needed to properly represent the complex concept of a force. (See 76).

158. In Chapter I, we saw that the sum of two vectors is the diagonal of a parallelogram whose adjacent sides are the two given vectors. Then the sum of two forces, or their resultant, is the diagonal of a parallelogram whose two adjacent sides represent the two given forces. Similarly, all the results obtained for vectors in that chapter hold equally well for forces. The condition for equilibrium of forces acting on a particle at the extremity of ρ is evidently $(\Sigma F)\rho=0$, or $\Sigma F=0$.

169. The formulas obtained in Chapter VI evidently hold true when the points are replaced by infinitesimal forces, as parallel forces acting on particles, and also when they are replaced by finite parallel forces. (See 80).

170. Let the resultant of the forces acting on a rigid body be denoted by R. Then if $\varepsilon=\rho-\rho_1$

$$R=\Sigma F\rho=\Sigma F\rho_1+\Sigma F(\rho-\rho_1)=(\Sigma F)\rho_1+(\Sigma F\varepsilon).$$

This result, called a "Wrench," contains two parts, a vector and a plane segment part. The vector ΣF represents the translation force, and the plane segment $\Sigma F\varepsilon$ gives the plane and magnitude of rotation. When the above result is interpreted geometrically, *i. e.* when ΣF is thought of as a line, and $\Sigma F\varepsilon$ as a plane segment, R is called a "Screw."